UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/691,361	10/21/2003	Jeffrey Bruce Lotspiech	ARC920030093US1	1410

28342 7590 02/22/2007

SAMUEL A. KASSATLY LAW OFFICE
20690 VIEW OAKS WAY
SAN JOSE, CA 95120

EXAMINER	
TRAN, ELLEN C	
ART UNIT	PAPER NUMBER
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/691,361	LOTSPIECH ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 February 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16,19-23 and 26-97* is/are pending in the application.

4a) Of the above claim(s) *16,19-23 and 26-97* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *21 October 2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: filed on 12 February 2007 with acknowledgement of an original application of 21 October 2003.

2. The application was subject to a restriction requirement, Applicant elected Group I of the restriction without traverse.

Claims 1-15 are rejected below; claims 1, and 8, are independent claims.

3. The IDS submitted 21 October 2003 been considered.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1-15,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Xu et al. US Patent No. 6,965,883 (hereinafter '883) in view of Alve et al. U.S. Patent Publication No. 2003/0076955 (hereinafter '955) .

As to independent claim 1, "A method for securely removing a device from at least one of a plurality of devices in a network, the method comprising:" is taught in '883 col. 14, lines 12-20 "Termination of the multicast session can happen either explicitly or implicitly. Explicit termination of the multicast session occurs when the user sends a disjoin request that specifies a stop time earlier than the pending stop time. A disjoin request is only effective, however, if group membership management 122 receives the disjoin request prior to the pending

stop time. Following receipt of a disjoin request, multicast charging unit 124 updates and closes the entry in charging database 126 and forwards the charging data to billing unit 171 for conversion into billing data and storage in billing database 172. If the forwarding of the charging data is successful, multicast charging unit 124 deletes the entry in charging database 126 and, if the second join request arrives after the first join status expires, multicast security unit 123 updates decryption key 118 for other group members of the same multicast session. Implicit termination of the multicast session occurs when the user's "joined" status expires before the user sends a subsequent join request to extend the stop time. An implicit termination may occur, for example, when the battery in the user's terminal loses power or some other reason that causes terminal to loose the network connection. Accounting for implicit termination of a multicast session ensures that an excessive charge does not accrue for the user";

"marking the device for removal, by modifying the list of the plurality of devices in the network; recalculating the encryption key using the modified list; and reencrypting the protected content with the recalculated encryption key" is shown in '883 col. 7, lines 4-16 "Group membership management 122 maintains the group membership information for every terminal on the same multicast link and is responsible for determining the join status of each terminal. Multicast security unit 123 is responsible for sending decryption key 118 to user terminal 110. Optionally, multicast security unit 123 may encrypt the multicast data from multicast server 190 before it is sent to user terminal 110. Multicast security unit 123 sends decryption key 118 when the user initially joins a multicast session. Multicast security unit 123 updates decryption key 118 either when another multicast user terminates the session or at discrete time intervals";

the following is not explicitly taught in '883:

"calculating an encryption key for a protected content in the network, based at least in part on a list of the plurality of devices in the network" however '955 teaches "An exemplary method includes receiving content at a user's device. The received content is encrypted with a content key. The content key is protected by encrypting it with a domain key. A user's compliant devices, or a family's compliant devices, can be organized into an authorized domain. All the devices in an authorized domain would have the ability to decrypt the encrypted content key. A user can freely send the encrypted content and the encrypted content key to other devices in the domain. At the receiving device, the content key is decrypted to its clear form. The clear content key is then available to decrypt the content. This assures content providers that their content will not be subject to widespread piracy because only devices within the user's domain can decrypt content keys encrypted with the domain key" on page 1, paragraph 0004, note the domain key is the calculated encryption key.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a charging mechanism for multicasting data to a home network taught in '966 to include a means to calculate an encryption key based on the list of devices currently in the network. One of ordinary skill in the art would have been motivated to perform such a modification because copy protection techniques need to enhanced for a home network see '955 (page 1 paragraph 0002). "Copy protection techniques exist in the prior art to address these issues. For example, the content can be tied to the user's device by encrypting the content with a key unique to the device. This approach, however, severely limits what valid licensed users can do with their content. Consumers expect to be able to have some freedom in the way they use their content.

They expect to be able to transfer the content to other devices they use; and, they expect to be able to make back-up copies to protect their content in the event of a hardware failure. Purchasers of music, for example, expect to be able to listen to the music they purchase at home, on their car stereo, and on portable audio devices. Accordingly, overly restrictive systems that prevent these types of uses are unlikely to be accepted in the marketplace".

As to dependent claim 2, "further comprising the device to be removed acknowledging its removal" is taught in '883 col. 14, lines 12-20, note if the device sends a message to be removed it is acknowledging its removal.

As to dependent claim 3, "further comprising denoting the acknowledgement in the modified list" is shown in '883 col. 7, lines 4-16.

As to dependent claim 4, "wherein recalculating the encryption key comprises including a key management block in the calculation" is shown in '883 col. 7, lines 4-16;

As to dependent claim 5, "wherein recalculating the encryption key comprises including an authorization table in the calculation" is taught in '883 col. 13, lines 45-55 " The join request sent by the user identifies the requested multicast session, the requested start time for the charging, and the requested stop time for the charging. The join request obligates the user to pay the charges that accrue from the start time to the end time. When the user has "joined" status, the multicast network is responsible for updating the user's "decryption key" whenever host membership in the multicast group changes. For a discussion of several methods for delivery of the decryption key see "Secure Group Communication using Key Graphs", IEEE/ACM Transactions on Networking, February 2000".

As to dependent claim 6, "wherein recalculating the encryption key comprises including the binding identification for the plurality of devices, excluding the device to be removed" however '955 teaches "The creation of the content key can be accomplished by randomly generating the key or by using a content key seed transmitted with the content. Sending a content key seed with the content allows the content provider to know the content key that will be used to encrypt the content without broadcasting the content key itself. The content provider accomplishes this by sending along with the content key seed a content ID. The content key seed and the content ID are associated with one another in a way known only by the content provider. Upon receipt of the content key seed an authorized device generates a content key by encrypting the content key seed with its domain key. After the content key is created the content key seed is discarded and no longer used by the receiving device. When the device creates a voucher associated with the content it includes in the voucher the content ID and a domain ID identifying its domain. If the content provider ever needs the content key, it can use the content ID and domain ID contained in the voucher to look up the content key seed and the domain key. It can then perform the same operation performed by the authorized device to recreate the content key" on page 4, paragraph 0042.

As to dependent claim 7, "wherein the protected content is encrypted with a title key; and further comprising reencrypting the title key with the recalculated encryption key" however '955 teaches "Referring to FIG. 5, the various authorized devices 12-16 in authorized domain 10 might all be manufactured by different entities. Accordingly, when a user of the domain adds a new device to the domain the trust management provider 500 can be consulted to certify that the new device meets the standards required by the system. This process

could include communicating with a third party that dictates the rules for domain creation for this user; e.g. a content provider. Alternatively, the trust management provider might control the entire process of joining devices into authorized domains and maintaining the created domains. In this role the trust management provider could also replace unusable content keys produced with content key seeds, as described above. The trust management provider might also provide information to the other devices in the domain concerning the operation of the new device" on page 6, paragraph 0071.

As to independent claim 8, this claim is directed to the system performing the method of claim 1; therefore it is rejected along similar rationale.

As to dependent claims 9-14, these claims contain substantially similar subject matter as claims 2-7; therefore they are rejected along similar rationale.

As to dependent claim 15, "wherein the plurality of devices comprise any one or more of: a television, a set top box, a personal video recorder, a video cassette recorder, a compact disk player, a compact disk player recorder, a personal computer, a portable music player, an audio player, a video player, a game console, and a personal network storage device" however '955 teaches any device to play or record content could be an authorized device on page 2, paragraph 0021.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
17 February 2007